UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/064,414	07/11/2002	Mong-Ling Chiao	ASIP0004USA	7464

27765 7590 04/07/2004

NAIPO (NORTH AMERICA INTERNATIONAL PATENT OFFICE)
P.O. BOX 506
MERRIFIELD, VA 22116

EXAMINER	
THOMAS, SHANE M	
ART UNIT	**PAPER NUMBER**
2186	4

DATE MAILED: 04/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/064,414	Applicant(s) CHIAO ET AL.	
	Examiner Shane M Thomas	Art Unit 2186	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-19 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-19 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 11 July 2002 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The disclosure is objected to because of the following informalities. In paragraph 38 of the Applicant's disclosure the element --10"-- (10 double-prime) should be corrected to --10'-- (10 prime) in order to maintain coherency with figure 4.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 1-5,7,8,10,12, and 15-17 rejected under 35 U.S.C. 102(a) as being anticipated by Cheng (U.S. Patent Application Publication No. 2002/0010827).

3. As per claims 1 and 15, Cheng shows a secure flash memory device 10 in figure 1, which comprises a connection port 1 to connect electrically to a computer; a --micro-controller-- (which the Examiner is considering as comprising micro-controller 3 and ROM 5) which is connected to the connection port 1; and a flash memory 4 electrically connected to the micro-controller (combination of 3 and 5). Cheng shows the functionality of a pre-installed security program in the secure flash memory device 10 in figure 4.

4. Because paragraph 28 of the Applicant's disclosure states that the security program prompts the user to enter a passcode, the Examiner is interpreting *a pass code stored in the computer* of line 10 to be dynamically stored in the computer (i.e. when the user inputs the pass code as a result of being prompted in accordance to paragraph 28). In other words, the Examiner is interpreting the pass code *stored in the computer* to be buffered by the computer when the user enters the pass code. Thus the pass code is not stored in the computer *before* the secure flash memory device is inserted into the computer's connection port. Steps 38 and 47 of figure 4 shows preventing a data exchange if the password input by a user does not match the predetermined code of the flash memory. If the password matches the predetermined code of the flash memory, the security program of figure 4 moves to either step 39 or 48 to allow access to the flash memory for reading or writing.

5. Further regarding claim 15, line 5, Cheng states in paragraph 18 that the security program is stored in ROM 5, which the Examiner is regarding as part of the micro-controller.

6. As per claim 2, a flash memory access request to a zone occurs in step 35 of figure 4, and the security program is run in order to verify that the password input by the user is correct.

7. As per claim 3, Cheng shows in figure 4 that the user has access two different partitions (zones) of the flash memory. Based on the partition the user selects for access in step 35, the security program determines how information can be exchanged between connection port 1 and each partition (zone 1 or 2) by following the respective steps of the selected zone as shown in figure 4.

8. As per claim 4, Cheng teaches in paragraph 19 that the predetermined code of user zone 2 can be set by the user. Figure 3 shows the procedure followed by the security program when changing the password.

9. As per claim 5, Cheng further teaches in paragraph 19 that the password entered by a user is encrypted.

10. As per claim 7, Cheng teaches in paragraph 19 that the passwords are typically stored in secure locations of the flash memory 4.

11. As per claim 8, as stated above, the Examiner is considering the ROM 5, which contains the security program of Cheng (¶18), as being part of the micro-controller. Therefore, the security program can be seen as being stored in the micro-controller.

12. As per claims 10, the Examiner is considering both the password to which an input pass code is compared to as well as the installation status flag [stored flash memory that confirms whether or not a password for zone 2's has been set by a user (paragraph 24)] as being collectively --a portion-- of the security program used to regulate accesses to the flash memory 4. Both the installation status flag and the zone passwords are integral --portions-- of the security program since the access cannot be granted to the flash memory if the correct password is not input and access cannot be granted to zone 2 of the flash memory if the password for zone 2 is not set (indicated by the installation status flag - step 35 of figure 4. Thus, it can be seen that a --portion-- of the security program which regulates the accesses to the flash memory 4 is stored in the flash memory (passwords for zones 1 and 2 - paragraph 19 - and installation status flag - paragraph 24) *and another* --portion-- of the security program is stored in the micro-controller (combination of elements 3 and 5) as discussed above.

13. As per claim 12, Cheng states in paragraph 17 that the connection port 1 is a USB connection port.

14. As per claim 16, the security program of Cheng (figure 4) prevents access to the flash memory as seen in steps 38 and 47. Refer also to paragraphs 25 and 27.

15. As per claim 17, if the password entered by the user equals the predetermined code, read/write access is allowed (steps 39 and 48 and paragraphs 26 and 28).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng (U.S. Patent Application Publication No. 2002/0010827) in view of Kobayashi et al. (U.S. Patent Application Publication No. 2004/0042363).

17. As per claim 6, the pass-code of zone 1 is input by a user, most often a software supplier as taught in paragraph 22 of Cheng. Cheng teaching using zone 1 to store applicant software to be accessible to a user upon entering the password for zone 1, most commonly the serial corresponding to the software on the secure flash memory device contained on the zone 1 of the flash memory 4. Cheng states that typically this predetermined password for zone 1 is stored in a secure location of the flash memory 4 (paragraph 19; hence the predetermined password for zone

1 is *not* stored in what the Examiner is considering to be a --micro-controller-- (combination of controller 3 and ROM 5). Kobayashi teaches in paragraph 32 that a ROM memory within a USB device can store the USB device's serial number. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have combined the secure flash memory device of Cheng with the teaching of Kobayashi in order to have been able to store the serial number (or zone 1 password) of the secure flash memory device in the ROM area 5 of the micro-controller. Because the zone 1 password would only have to have been written once (by the software supplier) and would never need to be changed (the USB device has a constant serial number), it would have been beneficial to store the serial number (zone 1 password) to read-only area of the ROM in order to have gained additional storage space in the flash memory (occupied by the serial number) and to further have the serial number of the device in a more secure location since users would not have had direct read access to the ROM 5 of the micro-controller.

18. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng (U.S. Patent Application Publication No. 2002/0010827) in view of Bean et al. (U.S. Patent Application Publication No. 2003/0074577).

19. As per claim 9, Cheng does not show storing the entire security program in the flash memory 4. Because the security program is primarily stored in the ROM 5 portion of the micro-controller, the security program is inaccessible to re-write feature such as to being updated by a firmware update feature. Such a feature could have allowed the security program of Cheng to have been updated if a bug was found to be in the code of the security program or if a new

version of the security program had been released by the manufacturer. Bean teaches a secure flash memory that stores a security lockout program in a flash memory 360 that is capable of being updated by virtue of a firmware upgrade (refer to paragraphs 57 and 58). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have combined the secure flash memory device of Cheng with the teaching of placing the security program completely within the flash memory of Cheng in order to have been able to have an authoritive source access the portion of the flash memory containing the security program for the purposes of upgrading the security program.

20. Claims 11 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng (U.S. Patent Application Publication No. 2002/0010827).

21. As per claim 11, Cheng states in paragraphs 25 and 27 that the user is required to select which zone to access and must input an appropriate password for both. Cheng does not specifically state that the interface used to input the password is a GUI but it would have been obvious to one having ordinary skill in the art at the time the invention was made to have used a GUI in order to have prompted a user to input a password so it would have been easier for the user to have seen when to input a password or select a zone.

22. As per claim 13, Cheng fails to teach the connection port 1 of figure 1 as being an integrated drive electronics (IDE) port. It would have been obvious to one having ordinary skill in the art at the time the invention was made to have used an IDE connection in the secure memory device of Cheng as IDE protocols are known to provide superior transfer rates to mass

storage devices than that of the USB protocol, thereby allowing faster accesses with a larger bandwidth connection.

23. Claims 14,18, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cheng (U.S. Patent Application Publication No. 2002/0010827) in view of Brandt et al. (U.S. Patent No. 5,892,905).

24. As per claims 14, 18 and 19, Cheng does not teach specifically using HTML as the programming language to code the security program. Brandt teaches in the abstract the HTML is a well-known language that can be used by any computer on the market today. Brandt further states that HTML is well-controlled and standardized language where new application features can be added as they are developed. This teaching would go hand-in-hand with the firmware upgrading as discussed in the rejection for claim 9. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to have written the security program of Cheng in HTML, in accordance to the teachings of Brandt in order to have been able to have had the software of the secure firmware device run on a wide variety of computers on the market.

25. Further regarding claim 19, Cheng shows a flash memory device in figure 1, which comprises a flash memory 14, a connection port 1, and a --micro-controller-- (combination of micro-controller 3 and ROM 5). ROM 5 of the --micro-controller-- is installed with the security program (paragraph 18), hence the Examiner is considering the security programs as being

installed into the --micro-controller-- since the Applicant never specifically states when or how the Applicant's security program is written into the memory of the Applicant's micro-controller.

26. Figure 4 shows the method of execution of the security program of modified Cheng, which accepts a pass-code (steps 37 and 46), compares the pass code with a predetermined pass code (steps 38 and 47), and based on the entered pass code, either allowed or restricts access to the flash memory device based on the comparison.

Conclusion

27. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure follows:

28. Mathers et al., (U.S. Patent No. 6,012,145) teaches using a flash memory, and IDE connection, and a micro-processor to regulate accesses to a portable hard disk drive as applicable to claims 1 and 15. Mathers further teaches in column 2, lines 3-9, that a BIOS serial number of the computer can be used as a password to authorize access to the data on the hard drive.

29. Cromer et al. (US Patent Application Publication No. 2003/0159056) teaches dividing portions of a bootstrap program for a security device into separate memories in paragraph 23 as applicable to claim 10.

30. Poo et al (Patent Application Publication No. 2003/0005337) teaches a mobile USB flash drive that uses biometrics as a security feature to prevent unauthorized accesses to the flash memory.

31. Estakhri et al. (U.S. Patent No. 6,385,667) teaches using a flash memory with variety of memory interfaces such as USB, PCMCIA, and IDE, as applicable to claims 12 and 13.

32. Chu (U.S. Patent No. 6,321,335) teaches using security features to prevent unauthorized access to a computer module.

33. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shane M Thomas whose telephone number is (703) 605-0725. The examiner can normally be reached on M-F 8:30 - 5:30.

34. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Matt M Kim can be reached on (703) 305-3821. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

35. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shane M. Thomas

MATTHEW KIM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100